

The Implications of the IRS Hack Are Worse Than You Think

Sara Williams October 21, 2015



In case you haven't heard, the IRS was well and truly hacked. This is one of the most frightening scenarios for the average American as there is nothing the IRS does not know about you.

([Newswire.net](#) -- October 21, 2015) -- Once IRS records are loosed, that is the end of data privacy as we know it. Here are some of the scarier implications:

You Need Better Data Security

The final, and most obvious implication to all this is that whatever security measures you are personally using, it is not sufficient. It is only a matter of time before individuals start turning to enterprise-grade security for their personal data.

Companies like Trend Micro offer security packages for both consumers and businesses. But when hackers can get into IRS records, the enterprise-level security starts to sound a lot more appealing.

If you have a small business, it is definitely time to upgrade to something more in the class of a [secure network](#). At minimum, your security solution will need to have the following:

- Comprehensive security capabilities, including anti-malware with web reputation, host-based firewall, intrusion detection/prevention, integrity monitoring, log inspection, encryption, application scanning, and globally trusted SSL certificates.

The Government Is No More Secure Than Any Other business

This is a real wake up call for everyone. We have been blinded by this comforting illusion that, while Big Brother may be annoying, imposing, intrusive, and downright scary, at least he knew what he was doing when it came to securing information. Now, we can no longer maintain that illusion. The government is no more secure than any other business vulnerable to hackers.

According to [Fortune](#):

Hackers accessed taxpayer information through the "get transcript" application, which allowed users to recall information that they input in previous tax returns. The system was shut down following the cyber attacks.

Not only was the IRS no better protected than anyone else, they were no better informed about the damage. The article goes on to say that the IRS grossly underestimated the number of attempts, and successful breaches to their systems. In part, the government's power is derived from the confidence people place in it. This hack seriously erodes that confidence.

It Lets the World Know that We Are Vulnerable

The last thing you want to do is let your enemies know where you are vulnerable. You want them to think that your armaments are irresistible, and your defenses are impenetrable. You never want to show them your weak underbelly.

We do not know for certain who is responsible for this hack, or how bad it really is. We are flailing about, desperately trying to find answers. Our impotence only serves to embolden our enemies to strike again, this time, at an even more tempting target, such as national defense.

As individuals lose confidence in the government to protect their data, they will start expecting more from you. So will credit card companies. [Target's data breach payout to Visa may hit \\$67 million](#) . That is because Target was thought to have acted irresponsibly when it came to data security. It makes it that much more important that you have the highest level of data security available for your business if you are dealing with the sensitive information of clients.

Ultimately, the implications are that we live in scary times. No system is completely secure. No company or individual is completely safe from being hacked. But for the maximum possible protection, we can do better. We must do better.

Source: <http://newswire.net/newsroom/pr/00090787-the-implications-of-the-irs-hack-are-worse-than-you-think.html>